Guest Editorial

Symposium issue on extraterritoriality and EU data protection

Cedric Ryngaert*

In a virtual world where in a split second data are transferred to and processed in far-flung corners of the world, national regulators may be at loss as to how to ground their jurisdiction. Indeed, due to these spatio-temporal shifts, the principle of territoriality, the traditional cornerstone of the law of jurisdiction, appears to be losing its salience in the field of international data protection. Where data are everywhere and become disconnected from physical territory, extraterritoriality may seem the only viable regulatory option. Unbounded extraterritoriality, however, has serious adverse consequences for both businesses and states. For businesses, regulatory burdens imposed by multiple states might increase transaction costs and legal uncertainty, while vigorous assertions of extraterritorial jurisdiction could cause international competency conflicts between different states, which might have different substantive views on the scope of data protection.

The quest for an appropriate jurisdictional nexus in international data protection is the subject of this special issue. It builds on a symposium on extraterritoriality and data protection organized at Utrecht University's School of Law on 6 May 2015, in the framework of the UNIJURIS project on the exercise of unilateral jurisdiction. A number of leading scholars in the field have been invited to shed light on how data protection jurisdiction could be reconceived in the current technological era of transnationally active data controllers and processors collecting, storing, controlling, and processing large amounts of personal data through technologies and processes that do not have strong territorial moorings. Contributors have been specifically requested to reflect on the geographical scope of EU data protection regulation. This choice of the EU is not accidental; as of all international actors, the EU has most zealously expanded the scope of its data protection regulation in an effort to provide protection to its citizens and residents whose data are transferred abroad and whose data are processed by foreign entities active on the EU market. Contributors have been asked to incorporate the transition from the EU Data Protection Directive (1995)[1] to the newly proposed EU General Data Protection Regulation.[2] Both legal instruments rely on territoriality, where they condition application of the relevant instrument on processing in the context of activities of a *territorial establishment*,[3] making use of *territorial equipment*,[4] offering goods or services to data subjects *in the EU*,[5] or monitoring behaviour taking place *in the EU*.[6] There is no denying, however, that these legal instruments, while formally based on territoriality, have extraterritorial effect, in that they affect foreign operators' data-controlling activities to the extent that they choose to be active on the EU market (even if only via an intermediary), or otherwise happen to control or process data belonging to EU data subjects. The EU Court of Justice's 2014 affirmation of EU data subjects' 'right to erasure' (under certain conditions) with respect to search results generated by US-based search engine Google,[7] and the resulting tug of war over the geographical scope of implementation of the judgment,[8] is one of the most conspicuous examples

* Professor of Public International Law, Utrecht University, School of Law, Achter Sint Pieter 200, 3512HT Utrecht, The Netherlands.
The UNIJURIS project is funded by the European Research Council under the Starting Grant Scheme (Proposal 336230—UNIJURIS) and the Dutch Organization for Scientific Research (NWO) under the VIDI Scheme. The editor of this special issue, C.R., extends his thanks to ERC and NWO for sponsoring the conference and the research time devoted to editing this special issue. The editor also extends his thanks to the editorial board of *International Data Protection Law*, and in particular to Professors Christopher Kuner and Dan Svantesson, for the opportunity to publish the papers of the conference in this special issue. Thanks to Mistale Taylor for her editorial assistance. This publication forms part of Utrecht University's Renforce research group's programme 'External Effects of EU Law'.

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 ('EU Data Protection Directive').

2 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM/2012/011 ('General Data Protection Regulation').

3 Article 4(1)(a) EU Data Protection Directive.

4 Ibid, Article 4(1)(c).

5 Article 3(2)(a) General Data Protection Regulation.

6 Ibid, Article 3(2)(b).

7 Case C-131/12, *Google Spain SL, Google, Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317.

of the extraterritorial effect of EU data protection law, and the controversy such effect can stir.

The various contributions to this special edition all touch upon issues of the overarching subject but are complementary at the same time. These are the main insights gathered from the contributions:

- The international law of jurisdiction is not very helpful when it comes to delimiting the geographical scope of a state or a regional organization's data protection legislation.[9] Public international law declares only the most outrageous jurisdictional assertions to be off limits. Insofar as the exercise of jurisdiction is based on one of the established permissive principles of jurisdiction, it will be presumptively lawful. The relevant jurisdictional provisions in data protection legislation, such as the aforementioned EU law provisions, do seem to be grounded in these principles, in particular territoriality (including the effects doctrine) and passive personality. As indicated above, EU data protection operates on the basis of EU territorial connections and effects and is aimed at protecting EU citizens and residents, or at least their personal data. As data controllers' activities have effects in, and affect citizens of, multiple states, multiple states will also have jurisdiction. This defeats the purpose of the classic principles of jurisdiction, the goal of which is precisely to *limit* the number of competent states, with ideally one state having exclusive jurisdiction over a particular state of affairs. More refined principles, tailored to the specific case of data protection legislation, may thus have to be contemplated. As Christopher Kuner argues in his contribution to this issue, an all-or-nothing approach to jurisdiction should be shelved, and calls for a serious inquiry into the appropriateness of specific jurisdictional assertions, taking into account the circumstances of the case and the level of protection offered abroad. New principles could possibly be tied to the protective purpose of specific provisions. In an earlier publication, Dan Svantesson has usefully distinguished between three layers of protection offered by different provisions in data protection legislation, with different legal consequences attached to each layer.[10]
- Under public international law, the lawfulness of a jurisdictional assertion is normally a function of the level of international (sovereign) protest voiced against the assertion on legal grounds. International conflict has arisen over the reach of data protection legislation, notably between the EU and the USA over, for example, EU passenger name record data submitted to the US Department of Homeland Security,[11] or over US access to an EU-based financial database for purposes of combating terrorist financing.[12] It is not clear, however, to what extent US concerns were informed by a conviction that EU extraterritoriality violates the existing principles of public international law. Thus, the outer bounds of legality of EU data protection extraterritoriality are inductively rather difficult to draw. Ultimately, the aforementioned conflicts were settled, at least temporarily, through international agreements. Other conflicts, however, are in the offing. One such example is the tension surrounding the application of US e-discovery orders to US corporations in respect of data held on foreign servers.[13] In data protection legislation, most protest does not come from states upset by other states' or the EU's extraterritorial antics, but from the data controllers themselves who are subject to extraterritorial regulation.[14] This mirrors the

8 B Van Alsenoy and M Koekkoek, 'The Extra-Territorial Reach of the EU's "Right to Be Forgotten"' (2015) ICRI Research Paper 20.

9 DJB Svantesson, 'The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on US Businesses' (2014) 50 Stan J Int'l L 53.

10 DJB Svantesson, 'A "Layered Approach" to the Extraterritoriality of Data Privacy Laws' (2013) 3 Int'l Data Privacy L 278 (distinguishing between the abuse prevention, rights, and administrative layer, with the most far-reaching consequences—possibly market-destroying measures—being attached to the first layer, which addresses unreasonable disclosure or other use of a subject's data).

11 See, eg Z Whittaker, 'EU Votes to Support Suspending U.S. Data Sharing Agreements, Including Passenger Flight Data', available at <http://www.zdnet.com/article/eu-votes-to-support-suspending-u-s-data-sharing-agreements-including-passenger-flight-data/> accessed 28 August 2015.

12 See, eg Spiegel, 'Online International, SWIFT Suspension? EU Parliament Furious About NSA Bank Spying' (18 September 2013), available at <http://www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920.html> accessed 28 August 2015, referring to the Agreement between the European Union and the USA on the processing and transfer of Financial Messaging Data from the European Union to the USA for purposes of the Terrorist Finance Tracking Program [2010] OJ L 8/11.

13 Cf. the search warrant served by the US Government on Microsoft under the Electronic Communications Privacy Act of 1986, authorizing the search and seizure of information associated with a specified web-based e-mail account stored on a Microsoft server located in Ireland.

14 See, eg the reaction of Peter Fleischer, Google's Global Privacy Counsel, to the French data protection agency's desire to implement the right to be forgotten on all versions of Google search, not only the French or European ones. P Fleischer, 'Implementing a European, Not Global, Right to Be Forgotten' (30 July 2015), available at <http://googlepolicyeurope.blogspot.nl/2015/07/implementing-european-not-global-right.html> accessed 28 August 2015. This is not to say that states always abdicate their responsibilities. In the aforementioned case of the search warrant served by the US Government against Microsoft, in an *amicus curiae* brief the Irish Government asserted that 'foreign courts are obliged to respect Irish sovereignty', thereby implying that the enforcement of the search warrant against data held on an Irish server violated international law. See *amicus curiae* brief of the Republic of Ireland, *Microsoft v US*, In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, Court of Appeal for the Second Circuit, 14-2985-CV, 23 December 2014. See also the view of the European Commission in V Reding, 'Letter to MEP In't Veld' (24 June 2014), available at <http://www.out-law.com/en/articles/2014/july/reding-us-authorities-wrong-to-ask-microsoft-directly-to-hand-over-customer-data-stored-in-the-eu/>

absence of strong reactions in the field of extraterritorial economic sanctions law, where affected businesses' home states have largely refrained from protesting against the adverse impact of extraterritorial sanctions.[15] Under state-centric international law as it currently stands, unfortunately perhaps, such non-state actor views have no direct impact on the legality of jurisdictional assertions, unless they are incorporated into state reactions.

- Controversies over the extraterritorial reach of data protection law are not simply clashes over which state should have proper jurisdiction. Underneath the jurisdictional discourse, dominated by such concepts as territoriality, effects, and personality, lies a more substantive discourse regarding the appropriate balance to be struck between data protection and other societal goals, such as security (for example, fighting terrorism or cybercrime) and facilitating transnational business.[16] The reactions to the right to erasure affirmed in the *Google Spain* judgement illustrate this well, pitting defenders of transparency, and the freedom of speech and information against defenders of individuals' right to be forgotten. Such substantive normative conflicts have traditionally played out at the domestic constitutional level, but they have become internationalized due to the transnational nature of the Internet and the attendant 'extraterritorial' regulatory interventions by government agencies. Given the plurality of values in international society, such transnational normative conflicts are difficult to solve. In this context, substantive harmonization of data protection law through, for instance, treaty law does not seem to be a viable option. A more promising avenue is for domestic or regional law enforcement agencies and courts to give due regard to rival views of foreign affected persons and states, for example, through broad-based consultations or *amicus curiae* briefs.[17] Having examined these views, regulators might refrain from applying their data protection legislation to the fullest extent and might possibly recognize foreign mechanisms that provide adequate or equivalent, although not identical, substantive protection.[18] This is any event how the safe harbour data protection framework developed by the United States Department of Commerce in cooperation with the European Commission works.
- That, in spite of the potentially broad geographical scope of data protection legislation, such legislation may not always be applied to its fullest extent factors in foreign sensitivities regarding extraterritorial overreach. It also reflects a realistic estimation of the options of *enforcing* assertions of extraterritorial prescriptive jurisdiction. Where data controllers have no establishment or assets in, or other links with the EU, such enforcement is difficult. The relevant controllers might not be inclined to take account of injunctions and penalties, although evidently, as a last resort mechanism, the asserting state or the EU may impede access to the territorial market. Opinion is divided over the effect of non-enforcement on the credibility of extraterritorial data protection law.[19] In this respect, it will be interesting to see how EU-based data protection agencies will enforce the right to erasure against a recalcitrant Google.
- Extraterritorial application of EU data protection legislation may differ from extraterritorial application of other legislation in that it pertains to an individual's *fundamental right*. The characterization of data protection law as fundamental rights law could have a bearing on the scope of the EU's jurisdiction, as the EU could, under certain circumstances, be *required* to protect persons falling within their jurisdiction. Under international human rights law, indeed, limited extraterritorial application may be given to human rights obligations, including provisions on data protection. It is not fully clear, however, to what extent it is incumbent on the EU to protect EU citizens' personal data controlled and processed abroad. While the EU, just like states, may be a duty-bearer in respect of the right to data protection,[20] it is open to debate

accessed 28 August 2015. ('The Commission remains of the view that where governments need to request personal data held by private companies and located in the EU, requests should not be directly addressed to the companies but should proceed via agreed formal channels of co-operation between public authorities, such as the mutual legal assistance agreements or sectorial EU-US agreements authorising such transfers.')

15 For example, for the Netherlands: <www.rijksoverheid.nl> accessed 28 August 2015, search for: doorwerking, sancties, Iran; for Belgium: <www.diplomatie.belgium.be> accessed 28 August 2015, search for: policy, peace and security, sanctions.

16 C Kuner, Transborder Data Flows and Data Privacy Law (2013) 135 (arguing that international conflicts over extraterritorial data protection are not just conflict of laws, but conflicts or 'normative collisions' between different social sectors and normative regimes).

17 See for the theoretical foundations of this 'other-regardingness': E Benvenisti, 'Sovereigns as Trustees of Humanity: On the Accountability of States to Foreign Stakeholders' (2013) 107 AJIL 295.

18 See on the use of mutual recognition as a jurisdictional safety valve: J Scott, 'The New EU "Extraterritoriality"' (2014) 51 Common Market L Rev 1343.

19 *Pro* DJB Svantesson, 'The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on US Businesses' (2014) 50 Stan J Int'l L 53 and Svantesson in this issue (implying that the moral justifiability of a jurisdictional assertion exerts a pull towards compliance, and distinguishing in this respect between bite and bark jurisdiction). *Against* C Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 2)' (2010) 18 Int'l J L & Info Tech 227, 235.

20 C Kuner (n 16), 130.

whether it has any protective duties towards EU citizens whose data have been transferred and processed abroad. Still, the law may shift here, also as a result of the international outcry following the abuse of extraterritorial surveillance techniques.[21] Mistale Taylor addresses this question in her contribution and argues that the EU is *obliged* to actively prevent third parties from violating the right to data protection in respect of data that are transferred outside the EU. EU or EU Member State regulators may discharge this obligation by preventatively entering into international agreements that require adequate protection, or by *ex post facto* bringing proceedings against foreign data controllers violating EU law (a fine example obviously being the *Google Spain* case).

- Where technology has enabled firms to do business generally unhindered by territorial boundaries, technology can at the same time be used to redraw territorial boundaries on the *prima facie* borderless Internet. Territoriality has indeed not entirely collapsed as a practical concept. States can use technology to block access to websites featuring undesirable (political) content[22] and potentially also to websites controlled by firms that insufficiently protect data of the state's citizens. Firms themselves can use geolocation technologies to prevent their websites from being accessed by viewers in certain jurisdictions with restrictive data protection laws. Where such firms have made a good faith effort to avoid a particular jurisdiction through technological means, but where its websites have nevertheless been consulted in that jurisdiction (for example, via virtual private networks), they can mount a persuasive defence that they have consciously not targeted that jurisdiction's citizens and thus should not be subject to its 'extraterritorial' data protection legislation.This special issue consists of four contributions that each addresses a different aspect of the extraterritoriality of EU data protection legislation, or at least of its jurisdictional reach.

Christopher Kuner takes issue with the confusing use of the terms 'territoriality' and 'extraterritoriality' in data protection law, and also more broadly in the law of jurisdiction. He submits that the EU legal framework applying to international data transfers (Articles 25 and 26 of the Data Protection Directive) necessarily has an extraterritorial dimension, as EU law requires that data protection standards in third countries be largely in accordance with EU law if data are to be transferred from the EU to these countries. In Kuner's view, it is more constructive to ascertain the *appropriateness* of extraterritorial assertions in practice. He calls on scholars and practitioners to determine the conditions of appropriateness. This equals abandoning the 'black-or-white' approach to the geographic application of EU data protection law (the law applies, or it does not apply). EU data protection law may instead not always apply in full, and boundaries may have to be set to prevent jurisdictional conflict with states that have other regulatory views or a stronger connection with the data controller.

Dan Svantesson argues that the distinction between territorial and extraterritorial jurisdiction in data protection should be abandoned and that instead such concepts as 'substantial connection', 'legitimate interest', and 'proportionality' should inform the jurisdictional analysis. Turning to the proposed EU General Data Protection Regulation, he takes issue with the 'targeting' approach embraced by the Regulation (that in its Article 3 provides that a non-EU-based controller falls within the Regulation's ambit where its processing activities are related to the offering of goods or services to EU data subjects) is misconceived, as in practice it may result in overbroad assertions of jurisdiction. According to Svantesson, often 'instances of data collection and processing will lack reference to the factors, such as currency, meant to determine whether the party targeted Europe or not', as a result of which the targeting approach is useless, possibly even giving rise to the quasi-automatic establishment of jurisdiction where goods or services are offered in the EU. Such data imperialism is undesirable, and an alternative, narrower jurisdictional approach is called for. Precisely how such an approach, which operationalizes the aforementioned non-territorial concepts, would look remains an open question.

While Kuner and Svantesson call for limits to the exercise of data protection jurisdiction, **Mistale Taylor** observes that the characterization of data protection as a fundamental right in the EU may *widen* rather than narrow the jurisdictional scope of EU data protection legislation. Indeed, the EU may have obligations to respect, protect, and fulfil its citizens' right to data protection also abroad, since human rights obligations may apply extraterritorially, as the European Court of Human Rights has held with respect to the European Convention

21 M Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 Harv Int'l L J 81, available at <http://ssrn.com/abstract= 2418485> accessed 28 August 2015.

22 See The Guardian, 'Google China: Inside the Firewall, Information Is in Short Supply' (23 March 2010), available at <http://www.theguardian.com/world/2010/mar/23/google-china-firewall-censorship-internet> accessed 28 August 2015; ibid, 'China Tightens "Great Firewall" Internet Control with New Technology', available at <http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control> accessed 28 August 2015.

on Human Rights. More specifically, this might mean that the EU is under an obligation to ensure that a data controller abroad does not violate an EU resident's right to data protection when this person's data are transferred abroad or otherwise in the hands of a foreign controller. It remains, however, that this long arm of EU data protection law could clash with the laws and interest of foreign nations, which may strike a different balance between data protection and other societal imperatives.

While most contributors focus on jurisdictional issues pertaining to the enforcement of EU data protection legislation by administrative authorities, **Maja Brkan** shifts the focus to *private enforcement claims* filed by data subjects against data controllers in civil courts. She concludes that the applicable legal framework under private international law does insufficient justice to data subjects' fundamental right to data protection, as the extant rules of jurisdiction provide obstacles to proper remedies. In order to remove these obstacles, she does not propose to amend the proposed EU General Data Protection Regulation, but rather to insert a new provision into the Brussels Regulation (recast) on jurisdiction, recognition, and enforcement of judgments in civil and commercial matters.[23] This Regulation already contains separate jurisdictional provisions for specific fields of the law. An additional provision could accommodate the specificities of data protection litigation, in particular the weaker position in which the data subject (similar to the consumer) will usually find herself. Such a provision could, among other things, provide that a data subject or an association representing her may not only bring proceedings against a controller or processor in the courts of the Member State in which the controller or processor is domiciled, but also in the courts for the place where the data subject is domiciled. This is provided that the controller or processor directs its activities to the data subject's Member State of domicile or to several States including that Member State. Accordingly, unlike Svantesson, Brkan does see merit in using the targeting approach for data protection jurisdiction purposes.

doi:10.1093/idpl/ipv025
Advance Access Publication 7 October 2015

23 Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L 351/1.